Technology Policy Update
21 November 2019
By Michael Kans, Esq.

House Judiciary Committee Continues Its Antitrust Examination

The House Judiciary Committee's Antitrust, Commercial, and Administrative Law Subcommittee continued its series of hearings titled "Online Platforms and Market Power" with an examination of the agencies charged with enforcing federal antitrust laws: the Department of Justice (DOJ) and the Federal Trade Commission (FTC).

Subcommittee Chair David Cicilline (D-RI) said the U.S. is experiencing a moment of extreme concentration across the economy as in industry after industry a few companies dominate critical markets that effect the day-to-day lives of hard-working Americans. He said unchecked by competition corporations can abuse their market power to raise prices for consumers, lower wages, and stifle entrepreneurship, and enriching themselves and their executives at the expense of everyone else. Cicilline said that one area where the concentration is most troubling is in the digital economy where a small number of dominant platforms have become critical intermediaries for the flow of commerce and information. He stated that while the platforms have delivered consumers some benefit, there is growing evidence that these platforms are now using their power to set the terms of the market in ways that enrich them but make it impossible to compete on an even playing field. Cicilline asserted that the news each day brings stories of how the decisions by these handful of companies increasingly determines whether a merchant, publisher, or app developer sinks or swims. He contended that because several of these monopolies operate business models premised on the surveillance of Americans, the power wielded over Americans is unprecedented.

Cicilline noted that six months ago the committee initiated a bipartisan investigation into competition in digital markets that follows in a long tradition of Congressional investigations into industry-wide assessments of whether dominant corporations were abusing their market power and whether U.S. laws are working to reverse the rising tide of economic concentration. Cicilline said the investigation is pursuing a similar path, and he said a key task for the subcommittee is understanding the enforcement record of each agency. Cicilline claimed that over the last decade alone, the largest technology firms have acquired over 436 companies, many of which were actual or potential competitors, but not a single transaction was challenged by antitrust enforcers. He added that only a handful were closely scrutinized. Cicilline said that the last major case brought by enforcers was Microsoft 20 years ago. He remarked that while these problems have plagued markets across the economy and not just in digital markets, the enforcement gap in these markets have created a de facto antitrust exemption for online platforms. Cicilline asked whether the federal agencies have failed to bring cases because of unfavorable caselaw requiring Congressional action to amend the law. He asked whether the inaction is due to a lack of agency resources or is it due to a lack of will at the agencies to enforce the laws on the books. Cicilline said that these are the questions the subcommittee is looking to answer through its investigation and areas he hoped would be fully addressed during the hearing.

Subcommittee Ranking Member James Sensenbrenner (R-WI) said in the course of ordinary oversight of antitrust enforcement agencies the committee conducts annual or biannual hearings to examine the waterfront before these important agencies, but the DOJ and FTC will discuss only one set of issues: antitrust issues in the tech sector. He asserted that the agencies understand the

importance of getting right the applicability of the nation's antitrust laws to this critical sector of the modern economy. Sensenbrenner noted that like the subcommittee, the agencies are in the midst of a searching inquiry into whether the U.S.'s century-old antitrust laws and government enforcement of those laws is adequate to the challenges presented by the new digital economy. Sensenbrenner said the subcommittee's examination thus far has looked at whether entities in the tech sector, particularly the largest online platforms, have or have not been accumulating and leveraging market power over competitors and other market participants. He added that affected entities include fellow technology companies, news publishers, and app developers who depend upon large online platforms to reach consumers and many others. He stated that the subcommittee has also examined aspects of online data privacy and the role online data plays in competition, particularly with very large accumulations of consumers' online data. Sensenbrenner said the testimony at the hearing would help the subcommittee by receiving the wisdom and expertise of the antitrust agencies and by helping legislators better understand if antitrust laws are current and up to the task of the modern digital economy. He added that there a number of issues before the agencies that Members are monitoring closely, including consent decrees. HE said he intended to submit questions for the record on situations where antitrust laws could be misapplied or extending to the point where success is punished, innovation is suppressed, and consumer welfare is harmed.

Committee Chair Jerrod Nadler (D-NY) stated that stated that "[t]here is growing evidence that a handful of dominant platforms now control key arteries of online commerce, content, and communications." He claimed that "[a] number of important digital markets are now dominated by just one or two firms. For example, Google controls over 90% of the global search market and Facebook captures over 80% of all global social media revenue…[and] [b]y some estimates, Amazon controls about half of all online commerce in the U.S." Nadler stated that "[w]hile the open internet has delivered enormous benefits to Americans, waves of anti-competitive consolidation in digital markets have had devastating effects on key elements of our democracy and economy, such as the free and diverse press." He said that "[i]t also threatens the survival of a key element of our economy—the American startup." Nadler stated that "[e]mpirical evidence suggests that the trends of increasing consolidation and market power in digital markets pose a threat to technology startups and innovation in the U.S. economy." He said that "[f]or example, it has been reported that seed funding for technology startups—the initial round of investment in a startup—has declined significantly from 2015 to 2018."

Nadler stated that "I am deeply concerned about the antitrust agencies' lax merger enforcement which has permitted these harmful levels of concentration and the rise of market power in the digital economy…[and] [i]n addition to rising consolidation, there have also been allegations of anti-competitive conduct in digital markets." He stated that "[f]or instance, as more small- and medium-sized businesses become reliant on the dominant platforms to reach customers, they have increasing concerns that discriminatory or exclusionary conduct by the platforms could destroy their business over the course of just a few days or months." Nadler stated that "[d]espite mounting evidence of illegal monopolization activities by the dominant platforms, and numerous cases brought by international enforcers, U.S. enforcers appear to be paralyzed." Nadler stated that "[i]t has been decades since the DOJ or the FTC has brought a significant monopolization case in the tech sector. " He said that "Tim Wu, a professor at Columbia University testified before the Judiciary Committee in July that the DOJ's court challenges against AT&T, IBM, and Microsoft 'were foundational in terms of shaking up industry and creating room for new firms to grow.'"

Nadler stated that "I am encouraged by reports of the agencies' current investigations into the dominant tech platforms, but the decline of enforcement over the past several decades is extremely

troubling—a decline, I should add, that has occurred across all industries, not just in the technology sector." He contended that "I find it hard to believe that companies have simply ceased engaging in illegal monopolization rather than the more likely explanation—which is that the agencies are underenforcing the antitrust laws." Nadler conceded that "[t]here may be a number of reasons for underenforcement by the agencies with respect to both anti-competitive conduct and merger review, including unfavorable case law, insufficient enforcement will, and inadequate agency resources, all of which I look forward to examining at today's hearing."

Nadler stated that "[o]ne problem Congress can most directly address is ensuring that the agencies charged with antitrust enforcement have sufficient funding…[and] [u]nfortunately, appropriations to these agencies have declined over the last decade despite an increase in merger activity and an increase in the complexity of investigations." He claimed that "[i]n real terms, agency funding in 2019 was nearly 20% lower than in 2010…[and] [i]t is vital that the antitrust agencies have the resources they need to do their jobs." Nadler stated that "[w]hile ultimately it is the responsibility of the antitrust enforcement agencies to enforce the law, Congress has an obligation to assess whether existing antitrust laws and competition policies—and the will to enforce those laws and policies—are adequate to address the competition issues facing our country, and to take action if they are found to be lacking."

Committee Ranking Member Doug Collins (R-GA) stated that "[t]he subcommittee's antitrust investigation has been one of the bright spots on the committee's agenda this term." He said "[t]he importance of digital technology to our constituents' lives grows every day…[and] [t]he tech sector is one of the greatest forces for innovation and wealth creation in the world and our economy." Collins claimed that "[r]arely in history have we witnessed such a transformative change in how we go about our lives." He stated that "[m]uch of that change is very much for the good, but not all…[and] [a]mong these changes are the ways that companies compete — both fairly and unfairly — to provide goods and services to consumers." Collins claimed that "[i]t is therefore critical that we work on a bipartisan basis to understand whether our current antitrust laws and our antitrust enforcement agencies are up to the task the tech sector presents." He remarked that "[w]e will have accomplished something important if together we can determine whether our antitrust laws need updating for the digital economy or whether the antitrust agencies need Congress' help to assure vigorous antitrust enforcement in the tech sector."

Collins claimed that "[f]rom the start of our inquiry, I have made clear the overarching principles guiding me in this endeavor:

- First, while some tech companies have become very big, big is not necessarily bad. Companies that offer new innovations, better solutions and more consumer benefits at lower prices often become big — to the benefit of society. Proposals to break up big companies because of their size alone risk throwing the baby out with the bath water and simply punishing success.
- Second, just like the existing antitrust laws, proposals for new legislation should aim to keep the free market free. Proposals to construct broad new regulatory regimes should be viewed with caution. Experience shows that regulatory solutions often miss the mark, solve problems less efficiently than free markets can and create new opportunities for anti-competitive companies to suppress competition through rent-seeking. That is especially true when regulation attempts to take on evolving problems in fast-moving markets.

Collins stated that "[t]his principle is particularly important to me as we seek a better way to protect the privacy of consumers' online data…[and] I announced in July of this year that I would be

introducing legislation this term to achieve better protection." He added that "I am working hard on that legislation and it is strongly animated by the principle I just laid out." He asserted that "[o]ther proposals, like laws adopted in Europe and California, threaten to entrench the market power of large incumbent tech companies under the cloak of protecting online data privacy…[and] I want us instead to enact a new federal law that better protects privacy without making it harder for new, small, innovative companies to enter the market, jostle with the giants and strive to become the blockbuster companies of tomorrow." Collins stated that "[t]he heads of the antitrust agencies before us today also have stated principles they believe should guide antitrust inquiries into the tech sector…[and] I look forward to hearing in depth today about their views and whether we can borrow from some of their guiding lights as we work our way through our own congressional inquiry."

FTC Chair Joseph Simons stated that

> New technologies can offer real consumer benefits, but they can also raise complex and sometimes novel competition issues. We have prioritized efforts to monitor, study, and, where necessary, bring enforcement actions to maintain competition in technology markets. We are undertaking these efforts not only in connection with the technology platforms that are the focus of this committee's ongoing investigation, but also with respect to technologies employed by companies throughout the economy that are changing and challenging competition. The FTC's Bureau of Competition this year announced a shift in internal resources to establish a Technology Enforcement Division, a dedicated group that will monitor competition in U.S. technology markets and recommend enforcement action when warranted.

Simons said that "[a]s outlined in [FTC] testimony from last month, current law provides the Commission with several potential avenues to counter anticompetitive conduct by large technology firms that seek to thwart nascent and potential threats by acquisition or other means." He stated that "[f]or instance, when evaluating mergers in dynamic markets, the Commission pays particularly close attention when an industry leader seeks to acquire an up-and-coming competitor that is changing customer expectations and gaining sales."

Simons claimed that

> The FTC is in the process of concluding a prominent policy initiative: its Hearings on Competition and Consumer Protection in the 21st Century. This extensive series of public hearings was convened to consider whether broad-based changes in the economy, evolving business practices, new technologies, and international developments warrant adjustments to competition and consumer protection law, enforcement priorities, and competition policy. The FTC worked to feature a wide variety of perspectives in these hearings. We invited legal and economic academics and consultants, public interest groups, public advocacy groups, 15 and representatives of businesses and industries to our hearing sessions. By the conclusion of our final hearing on June 12, 2019, we had convened 14 sessions over 23 days, with thousands of people attending via webcast or in person. To date, we have received close to 950 unique comments on the covered topics. All the information related to the hearings—the transcripts, comments, presentations, and questions—is available on the FTC website. This large corpus of material on the critical issues facing modern competition and consumer protection policy has already created a valuable resource for future research by the agency, interested academics, practitioners, and policymakers. At this stage, we are

> distilling the large volume of stakeholder input and generating further output, such as reports, statements, guidance, and speeches.

Simons stated that

> As we have previously announced, we are prioritizing work involving platform competition, vertical mergers, and international initiatives. This work will be forward-looking and will both support the Commission's enforcement mission and identify additional policy initiatives that may be important in shaping the future development of antitrust law. We expect to begin releasing some of this output soon. Through these hearings, the Commission intends to help formulate an enduring approach to current questions about antitrust and consumer protection enforcement. We recognize that, in some areas of the law, some now question the policies that have served as the basis for what had long been a bipartisan consensus. Particularly with respect to certain antitrust issues where this consensus has been questioned, we believe these hearings were a valuable investment of our resources to determine whether adjustments are necessary.

Assistant Attorney General Makan Delrahim said the Antitrust Division at the DOJ is hard at work reviewing the business practices of online platforms, which was announced in July. He said to date both Facebook and Google have publicly disclosed investigations. Delrahim stressed those companies are not the only focus of the review but they are a significant part of the review because of the role they play in the lives of so many American citizens. He added these companies occupy a unique role in the era of online, personalized advertising supported by user data. Delrahim said the work the DOJ is doing is focused in part on understanding the role data play in personalized advertising and the competitive dynamics. He stated DOJ is looking at how these dynamics create value for advertisers, content creators, and the consumers who use these advertising supported platforms. Delrahim claimed that by understanding these competitive dynamics, the DOJ can determine if the market leaders have monopoly power, how they exercise such monopoly power, and whether the source of that power is from merits-based competition or if the source of that power is exclusionary or anticompetitive conduct. Delrahim stated that other online platforms make money in other ways, and we're reviewing those other business models as well. He contended that the common thread is that online platforms bring together users who access information services on the platform with third party providers of products, services, or advertisement. Delrahim claimed the DOJ is concerned about ways the online platform operators can manipulate the conditions for competition, and in some instances, the platform operators may have the incentive to improve the platform for the benefit of all those users while in other instances the platform operator may compete against users of the platform and may have an incentive to disadvantage competitors. He noted the DOJ's 2008 action against Google and Yahoo's agreement that would have eliminated the latter as an online search engine, and the companies ultimately decided not to proceed. Delrahim stressed he could not comment on the ongoing investigation but recent public remarks should assure the committee that the DOJ is taking a hard look at any possible anticompetitive behavior in online markets.

Hearing on Big Tech's Impact on Small Businesses

The House Small Business Committee held a hearing titled "A Fair Playing Field? Investigating Big Tech's Impact on Small Business." In a memorandum, Democratic staff claimed

> The Internet and information and communications technologies (ICT) have transformed American lives and spurred explosive economic growth by making instant communication seamless and intuitive. This is due, in large part, to the birth of powerful digital platforms, commonly referred to as Big Tech, that connect consumers to businesses in exceedingly efficient and innovative ways. However, the pervasive integration of Big Tech platforms and their near exclusive ability to direct online traffic has raised significant questions about the impact of Big Tech's influence on consumers and small businesses. As a result, policymakers are considering ways to empower and protect platform users.

Chair Nydia Velasquez (D-NY) thanked Amazon and Google for choosing to appear before the committee, which was not an easy decision for the companies but in her view the correct decision. She noted that two empty chairs at the witness table for Apple and Facebook, two companies with the means to spend millions on lobbying and corporate executives but cannot send representatives to the hearing. Velasquez said the companies' failure to appear not only impedes Congress' mission but also says volumes about transparency and their views on their customers. She again thanked Google and Amazon for appearing and said of Facebook and Apple "you reap what you sow."

Velasquez said the committee held a hearing earlier this year on how the digital ecosystem promotes entrepreneurship and held a roundtable last year with Amazon on Prime Day. She asserted that both events showcased the benefits tech platforms provide small businesses. Velasquez said the committee will look at the issue through another lens. She remarked that innovation and ingenuity built the U.S. and claimed one could argue these qualities are uniquely American. Velasquez added the qualities have propelled the U.S. to produce both the foremost companies and technologies.

Velasquez claimed that the grip that big tech now holds over American's daily lives and the U.S.' competitive landscape is both astounding and concerning. She argued that big tech platforms dominate search functions, the devices used by nearly every American, online advertising, and online messaging platforms. She added they are market leaders in cloud computing services to businesses and consumers while also providing entertainment and digital streaming services. Velasquez said that Microsoft, Apple, Amazon, Alphabet, and Facebook are collectively worth over $4.3 trillion and comprise over 15% of the total volume of the S&P 500. She said to provide further context on the scope and reach of these companies, Amazon currently has 50% of the U.S. e-commerce market, nearly 90% of internet searches go through Google and its subsidiary YouTube, Facebook pulled in $55 billion in ad revenue last year, and in 2018 alone, Apple sold over 217 million iPhones. Velasquez said that the sheer size of the companies along with the integration of their platforms and concentration of power influencing online traffic raises questions to anyone who cares about market access, data privacy, small business development, entrepreneurship, and innovation.

Velasquez asserted one need only look at the decline in American startups to connect the dots. In 2006, 558,000 businesses were formed but in 2015 the number was 414,000. She claimed there is growing anxiety not only in U.S. but around the world that the large tech companies pose a threat to innovation and competition. Velasquez noted that when consolidation takes place in any industry, market power is increased as it has in the tech industry. She added that thereafter it is simply too hard for new businesses to get off the ground. Velasquez said that many of the popular products and features of these companies have not been developed internally and rather were acquired through mergers and acquisitions with the largest being Microsoft paying over $26 billion for LinkedIn. She asked if the U.S. wants to be a country of entrepreneurs and investors that dream of

building something or dream of being bought by larger competitors. Velasquez declared that the U.S. needs to reboot the startup economy. She contended that when startup companies do get off the ground, the U.S. must ensure they are treated fairly in online marketplaces and that consumers can find them on search engines. She claimed that small businesses need certainty and transparency when they are operating their businesses on digital platforms so that they can set competitive prices and still make enough money to continue to grow their businesses, create jobs, and invest in their communities. She stated that when small firms do get into disputes with the powerful gatekeepers, they need a fair shot at resolving the problem so they can continue to run their businesses.

Velasquez said in closing that the data of the American people is an economic asset, which garners more value as one collects more of it. She claimed the concentration of data in fewer and fewer firms has implications for small businesses. Velasquez said the internet and digital platforms are so deeply woven into Americans' lives that small firms cannot afford to be excluded or treated unfairly. She asserted that small businesses need to be protected by policies that offer them the certainty and transparency they need to make meaningful business decisions. Velasquez stated that as consumers continue to increase their engagement with businesses through digital platforms, small businesses need to be sure they can be found when new and existing customers are looking for their business.

Ranking Member Steve Chabot (R-OH) thanked the witnesses for appearing because he understands it is not always easy for witnesses to take time out of busy schedules to testify. He asserted the digital age has caused a revolution for small businesses and no longer are smaller firms caught behind their larger counterparts when it comes to the availability of game-changing technologies to help grow and expand their businesses. Chabot claimed small firms can now utilize cutting edge products and services to respond to market changes very swiftly. He claimed that with the adoption of mobile computing devices, cloud systems, and online conference calls, employees can collaborate effectively across great distances and work almost anywhere. Chabot said the biggest benefit may be the financial savings it affords small businesses as increases in productivity allow small businesses to do more, faster and with less overhead. Chabot stated that it is no surprise that many of these platforms have been developed and marketed by many of the large tech forms. Chabot conceded there have been some concerns regarding privacy and intellectual property but, by and large, the development of these digital platform products and services from these tech giants has been a boon for the millions of individual small businesses that would probably never have existed without them. He said the hearing is an opportunity to examine the relationship between small firms and big businesses. Chabot claimed both needed each other to continue "our unprecedented economic expansion of the past three years."

Grow with Google's Head of Community Engagement Erica Swanson asserted

- The growth of the digital economy is providing enormous opportunities for small businesses to reach new customers. Google helps with this through our free products and services as well as our paid advertising services. I'd like to highlight three main ways our products support the success of small businesses: by providing discoverability on Google Search and Maps, by helping them to reach new customers through our advertising products, and by enabling them to run their businesses more effectively with productivity tools.
- Connecting with new customers is the number one need for small businesses. Every online interaction is an opportunity to find new customers and win their loyalty. Being discoverable online is critical -- 83% of U.S. shoppers who visited a store in the last week said they

searched online first. Each one of these searches is an opportunity for a small business to reach a new customer or re-engage an existing one.

- Businesses are discoverable on Google not only in "organic" Search — the standard, non-advertising search results — but also through free Business Profiles on Google, where businesses can list their websites, add photos, update hours, and more. These free tools help small businesses gain exposure online. When people see a complete Business Profile on Google Search and Maps, they are 50% more likely to buy something. Business Profiles also allow business owners to respond to user reviews, to build customer loyalty, post updates such as a discount or a promotion, and to generate excitement and drive sales.
- In addition to free services, we have a robust suite of advertising products to help small businesses reach the right customer at the right time. Through Google Ads, Google connects many potential customers to small businesses via the clearly-labeled sponsored ad placements above and below the search results on Google.com, as well as across our other properties, partner sites, and apps. To use Google Search ads, small businesses create short text ads and bid in an online auction for the keywords they want their ads associated with. A coffee shop, for instance, might bid on the phrase "cafe in Nashville. " When someone searches for this or a related phrase on Google, they may see the coffee shop's ad above or below the search results. The business only pays when someone clicks the ad to visit their website. For every $1 invested in Google Ads, our estimates suggest that businesses make an average of $2 in revenue. For service businesses — such as plumbing and housekeeping companies — we offer Local Services ads, which are designed specifically to help them connect with local customers looking for such services. And with Google Analytics on a business's website, the owner can better understand her customers to make her online marketing efforts even more effective.
- Additionally, Google's suite of workplace productivity tools, G Suite, helps small businesses work more efficiently so that they can scale and succeed. From organizing to planning, many small businesses spend a significant portion of their time managing back-office tasks. 77% of small businesses say they are looking for ways to save time at work. G Suite does exactly that by giving small business owners a custom, professional-looking email address (like joe@yourcompany.com), an easily shareable calendar, and secure cloud storage so users can create and access documents and spreadsheets from anywhere. And if a business has an online store, it can add Google Pay to simplify checkout. Google Pay gives customers a faster, safer way to pay that's free to both the business owner and customers.

Amazon's Customer Trust and Partner Support Vice President Dharmesh Mehta contended:

- U.S. small businesses are thriving on Amazon: on average, they sell more than 4,000 items per minute in our stores. In 2018, small and medium-sized businesses made an average of $90,000 selling in Amazon's stores. More than 50,000 entrepreneurs surpassed $500,000 in sales and 25,000 of them exceeded $1 million. We are also incredibly proud of the fact that small and medium-sized businesses selling in Amazon's stores have created more than 830,000 jobs in the U.S.
- When Amazon first invited third parties to start selling on Amazon in 1999, they represented just 3 percent of our sales, totaling $100 million. Amazon invested substantially and invented products and services to empower selling partners to help them succeed. Now, over 58 percent of the value of physical products sold in Amazon's stores come from small and medium-sized businesses – totaling $160 billion. Third-party sellers' compound annual growth rate has been 52 percent over the past 19 years, while our first-party business has grown 25 percent. To be clear, that means that third-party sales are growing more than

twice as fast as Amazon's own sales. We celebrate that growth, and we expect that trend to continue.

- In addition to helping small and medium-sized businesses sell in our stores, we've created a series of services and opportunities that enable businesses and entrepreneurs of all kinds to pursue their dreams by opening access and bypassing traditional gatekeepers:
    - Hundreds of thousands of authors have self-published millions of books through Kindle Direct Publishing. This means more diversity of authors, a broader range of content, and ultimately better products for our customers.
    - We are empowering independent contractors to partner with Amazon in fulfillment operations and become business owners. As business owners, they hire and develop a team of drivers employing up to 100 people and operate a fleet of vans. Amazon helps them get set up and ready to operate out of a delivery station in their local city.
    - Hundreds of thousands of small and medium-sized businesses, tech consultants, and startups use Amazon Web Services (AWS). In 2018, we provided more than $500 million in AWS credits to help startups build their business.
- Alexa gives entrepreneurs the opportunity to reach millions of engaged customers with a voice-first business. More than 90 percent of new Alexa-enabled products are built by someone other than Amazon. Hundreds of thousands of third-party developers have built more than 100,000 Alexa skills.
- These services, tools, and opportunities enable a wide variety of selling partners, content creators, and independent merchants to sell their products, fuel their creative passion, and grow their businesses – all of which helps drive the U.S. economy.

Viahart Toy Co. CEO Molson Hart asserted

- To the question "Has Amazon created business solutions that have enabled small businesses to reach and serve new customers?" - The answer to that question is "Yes, absolutely." Their Fulfillment by Amazon program solved logistical issues for small businesses that previously would've required big investments or big headaches. This has enabled small businesses to offer less expensive and innovative products more easily to American consumers. Everyone, perhaps with the exception of brick-and-mortar retailers, has won: Amazon, small businesses, and consumers. As a result, Amazon owns e-commerce. We can talk statistics, but just trust me; for most categories, such as books, toys, electronics, home goods, and gifts etc., basically everything but cars, food, gasoline, luxury, and convenience, Amazon is dominant. In 2018, despite selling on eBay, Walmart.com, our own website, and brick and mortar stores, Amazon accounted for 98% of our revenue.
- So, "Do small businesses like ours rely on Amazon?" Yes, completely. When they say "jump", we say "how high" - if Amazon suspends us from the platform, we go bust, and we go bust fast. In 2018, we paid $2 million dollars to Amazon and Amazon's expenses as a share of our revenue on Amazon have gone from 33% in 2013 to 50% in 2018. That said, we've been profitable and our sales have grown 37% every year over that period.
- So "Do small businesses have an opportunity to compete in the information age?" It is not easy and we work very hard, but we, as a small business, have done all right. So, yes, we do have an opportunity to compete amongst "Big Tech"...but, is the playing field fair? The answer to that is like a Facebook relationship status - "it's complicated". If we compete against Amazon, we operate at a massive disadvantage, but provided they don't engage in underhanded tactics, that's okay. It's capitalist competition. If Amazon Basics knocks off

one of our products, provided they didn't commit IP infringement, it's unfortunate, but it's okay.

Public Knowledge Senior Vice President Harold Feld stated that "Congress has historically moved cautiously in expanding sector specific regulation…[and] [o]ur recommendations are therefore designed to work individually as well as in combination:

- *Data portability*. One important feature in digital platform dominance is the collection and use of personal data from customers. This is particularly important for small businesses trying to maintain relationships with customers. Requiring platforms to honor requests from customers to move data to other platforms in usable formats has been recommended by many experts as a way to enhance competition. In the small business context, it would enable customers to move information from the platform to the small business if the customer chooses, decreasing dependence on the platform intermediary, in addition to moving information to businesses that directly compete with the platform.
- *Open APIs, licensing essential patents, and interoperability*. Public Knowledge proposes eliminating significant barriers to interoperability for competitors and for businesses using a platform as an essential input. For example, content creators should be able to use the same applications to create content for diverse platforms such as YouTube, Twitch and Facebook without worrying that one of the important platforms will take steps to force them into proprietary applications. The history of the telecommunications industry shows that interconnection creates competition and creates stability for small businesses, since they can use interconnected competitors to access reliably their customers on competing platforms. For the same reason, Public Knowledge recommends that companies that hold patents or copyrights that are essential to industry standards be required to license their intellectual property on fair, reasonable and non-discriminatory terms (FRAND). This does not mean that intellectual property holders must make their IP available for free. But FRAND licensing has been an important tool to prevent firms from using their IP to freeze out potential competitors or impose terms that prevent others from developing new, disruptive business models.
- *Restricting use of information collected from commercial rivals and prohibiting "most favored nation" clauses.* Public Knowledge therefore proposes measures that have demonstrated effectiveness in the communications market. First, Public Knowledge proposes limitations on the use of proprietary information collected by the platform as part of its business dealings with small businesses. This type of information is known in communications law as "customer proprietary network information" (CPNI). CPNI recognizes that although the network must "know" certain types of highly proprietary information to function, the law can limit the ability of the rival network to use this information for purposes other than the contracted service. Second, Public Knowledge proposes prohibiting punitive MFN clauses, or other mechanisms that prevent small businesses from finding alternatives to the dominant platform. Allowing small businesses to move freely between platforms without fear of reprisals is critical to maintaining a competitive environment and limiting the ability of dominant platforms to abuse small businesses dependent on them. It also promotes the development of competition, since dominant platforms cannot use their market power to prevent small businesses from patronizing rivals and enhancing their likelihood of success.
- *Non-discrimination, transparency and 'black box testing.'* Where a party has reason to believe that search and recommendation results are manipulated to discriminate in an inappropriate fashion, the party would file a complaint with the enforcing agency. The enforcing agency would then be given access to the code for testing purposes. The enforcing agency would then determine whether or not reasonable grounds exists to open an investigation. The complaining party would not get access to the code, thus avoiding the

ability of parties to use the complaint process as a pretext to gain access to proprietary algorithms to reverse engineer them.

- *Product unbundling and structural separation*. Structural separation and unbundling can be a very effective means of introducing competition and providing a level playing field for small businesses. The difficulty of implementing these regimes, however, should not be underestimated. Both structural separation and unbundling require ongoing regulatory supervision to ensure that the platform follows the rules. While the need for pervasive monitoring and supervision can be reduced in a well-designed system, it cannot be wholly eliminated as the economic factors that drove the consolidation in the first place will, absent some countervailing force, drive the separated pieces to reconsolidate.
- *Break ups and the Starfish problem*. Tear up a starfish and it simply regrows the missing limbs. While not all monopolies suffer from the starfish problem, this natural regeneration of concentration will occur in any market where the underlying economic structure of the market itself drives toward concentration. For this reason, although vigorous antitrust investigation and enforcement against dominant platforms is necessary, even the largest platforms can not simply be broken into pieces as a means of solving existing competition problems. Before any break-up, Congress must carefully consider what regulatory framework will prevent the market from simply returning to its highly concentrated state.

U.S.-China Commission Releases Annual Report

The U.S.-China Economic and Security Review Commission (Commission) has released its annual report, and not surprisingly the technological relationship between the two nations featured prominently in its findings and recommendations. However, the annual report presents a comprehensive picture of the relations and interactions between the two countries that will inform the broader debate in Washington on how best to address China's rise and how the U.S. should respond, especially in the economic and trade sphere. The Commission explained that "[t]his Report responds to our mandate "to monitor, investigate, and report to Congress on the national security implications of the bilateral trade and economic relationship between the United States and the People's Republic of China."

The Commission explained that:

- In 2019, the trade dispute between the United States and China entered its second year and remains mostly unresolved. The Chinese government's unwavering commitment to state management of its economy remains a major stumbling block. In response to de-cades of unfair economic practices, the United States wants the Chinese government to codify commitments to strengthen intellectual property protection, prohibit forced technology transfer, and remove industrial subsidies. But these practices are core features of China's economic system, and the Chinese government views U.S. demands as an attack on its national development. China continues to ignore the letter and the spirit of its World Trade Organization (WTO) commitments. The resulting impasse has led to multiple rounds of mutual tariff actions impacting more than $500 billion in bilateral goods trade, and reducing trade between the two countries. In response to U.S. measures to address illegal activities of Chinese technology firms, China's government strengthened pursuit of technological self-reliance and its state-led approach to innovation, which uses licit and illicit means to achieve its goals. This will continue to pose a threat to U.S. economic competitiveness and national security.
- Escalating trade tensions with the United States compounded China's domestic economic challenges, with the Chinese economy growing at its slowest pace in nearly 30 years in

2019. High debt levels constrain Beijing's ability to respond to the slowdown, and stimulus measures have so far been modest in comparison with past programs. The economic slowdown has disproportionately affected China's small and medium enterprises, which do not enjoy the same preferential treatment, access to credit, and government subsidies as state-owned or -supported enterprises. Meanwhile, regional banks have emerged as a key source of risk in China's financial system due to the high number of nonperforming loans on their balance sheets. China's government has also pursued limited market and financial system opening over the last year in an effort to attract foreign capital. These measures remain narrowly designed to address specific pressures facing China's economy and do not appear to herald a broader market liberalization of the kind that U.S. companies and policymakers have long advocated.

Regarding the technology-related findings, among the Commission found:

- On-and-off trade negotiations between the United States and China to resolve a years-long trade dispute have failed to produce a comprehensive agreement. The impasse in negotiations underscores, in part, China's commitment to preserving the government's dominant role in determining economic outcomes.
- The United States is confronting China in response to decades of unfair Chinese economic policies and trade-distorting practices. The Chinese Communist Party (CCP) increasingly perceives U.S. actions as an attack on its vision for China's national development. China's government has intensified nationalist rhetoric criticizing the United States, applied pressure on U.S. companies, and targeted key U.S. export sectors with tariffs in response.
- U.S. measures to address illegal activities by Chinese technology companies are leading China's government to push harder on technological self-reliance. The reinvigoration of the state-driven approach to innovation will pose a sustained threat to U.S. global economic competitiveness and national security.
- Beijing views its dependence on foreign intellectual property as undermining its ambition to become a global power and a threat to its technological independence. China has accelerated its efforts to develop advanced technologies to move up the economic value chain and reduce its dependence on foreign technology, which it views as both a critical economic and security vulnerability.
- The nature of Chinese investment in the United States is changing. While Chinese FDI in the United States fell in 2018, VC investment in cutting-edge sectors has remained more stable. Broad trends in FDI from China mask VC investment. While lower than FDI, VC investment from Chinese entities could have more impact as it has prioritized potentially sensitive areas, including early-stage advanced technologies. This sustained Chinese investment raises concern for U.S. policymakers, as Beijing has accelerated its comprehensive effort to acquire a range of technologies to advance military and economic goals.
- U.S. laws, regulations, and practices afford Chinese companies certain advantages that U.S. companies do not enjoy. Chinese firms that raise capital on U.S. stock markets are subject to lower disclosure requirements than U.S. counterparts, raising risks for U.S. investors. The Chinese government continues to block the Public Company Accounting Oversight Board from inspecting auditors' work papers in China despite years of negotiations. As of September 2019, 172 Chinese firms were listed on major U.S. exchanges, with a total market capitalization of more than $1 trillion.
- China's laws, regulations, and practices disadvantage U.S. companies relative to Chinese companies. China's foreign investment regime has restricted and conditioned U.S. companies' participation in the Chinese market to serve industrial policy aims. In addition, recent reports by the American and EU Chambers of Commerce in China suggest technology

transfer requests have continued unabated. Technology transfer requests continue to compromise U.S. firms' operations.

- Chinese firms' U.S. operations may pose competitive challenges if they receive below-cost financing or subsidies from the Chinese state or if they can import inputs at less than fair value. There are serious gaps in the data that prevent a full assessment of the U.S.-China economic relationship. Analysis of Chinese companies' participation in the U.S. economy is constrained by the absence of empirical data on companies' operations, corporate governance, and legal compliance.
- China's government has implemented a whole-of-society strategy to attain leadership in AI, new and advanced materials, and new energy technologies (e.g., energy storage and nuclear power). It is prioritizing these focus areas because they under- pin advances in many other technologies and could lead to substantial scientific breakthroughs, economic disruption, enduring economic benefits, and rapid changes in military capabilities and tactics.
- The Chinese government's military-civil fusion policy aims to spur innovation and economic growth through an array of policies and other government-supported mechanisms, including venture capital funds, while leveraging the fruits of civilian innovation for China's defense sector. The breadth and opacity of military-civil fusion increase the chances civilian academic collaboration and business partnerships between the United States and China could aid China's military development.
- China's robust manufacturing base and government support for translating research breakthroughs into applications allow it to commercialize new technologies more quickly than the United States and at a fraction of the cost. These advantages may enable China to outpace the United States in commercializing discoveries initially made in U.S. labs and funded by U.S. institutions for both mass market and military use.
- Artificial intelligence: Chinese firms and research institutes are advancing uses of AI that could undermine U.S. economic leadership and provide an asymmetrical advantage in warfare. Chinese military strategists see AI as a breakout technology that could enable China to rapidly modernize its military, surpassing overall U.S. capabilities and developing tactics that specifically target U.S. vulnerabilities.
- New materials: Chinese firms and universities are investing heavily in building up basic research capabilities and manufacturing capacity in new and advanced materials, including through acquisition of overseas firms, talent, and intellectual property. These efforts aim to close the technological gap with the United States and localize production of dual-use materials integral to high-value industries like aerospace. They could also enable China to surpass the United States in applying break- through discoveries to military hardware.
- Energy storage: China has quickly built up advanced production capacity in lithium-ion batteries and established control over a substantial portion of the global supply chain, exposing the Unit- ed States to potential shortages in critical materials, battery components, and batteries. China's heavily subsidized expansion in lithium-ion batteries will likely lead to excess capacity and drive down global prices. If Chinese producers flood global markets with cheaper, technologically inferior batteries, it would jeopardize the economic viability of more innovative energy storage technologies currently under development in the United States.

Among the technology-related recommendations the Commission made are:

- Congress direct the U.S. Department of Justice to reestablish a higher education advisory board under the Federal Bureau of Investigation. In concert with the U.S. Department of Commerce's Bureau of Industry and Security, U.S. Department of Homeland Security, and

U.S. Department of State, the higher education advisory board would convene semiannual meetings between university representatives and relevant federal agencies to review the adequacy of protections for sensitive technologies and research, identify patterns and early warning signs in academic espionage, assess training needs for university faculty and staff to comply with export controls and prevent unauthorized transfer of information, and share other areas of concern in protecting national security interests related to academic research.

- Congress direct the U.S. Government Accountability Office to conduct an assessment on the risks posed by Beijing's efforts to co-opt foreign researchers or students at U.S. universities to unlawfully appropriate research and other knowledge for the benefit of the government, companies, or interests of the People's Republic of China. This report should:
    - Include the number of foreign students and researchers from China studying in science, technology, engineering, and mathematics fields; past and current affiliations; primary areas of research; duration of stay in the United States; and subsequent employment;
    - Identify whether federally funded university research related to emerging technologies may have been unlawfully appropriated by individuals acting on behalf of Chinese entities; and
    - Evaluate the efficacy and ability of the U.S. Department of State's visa screening mechanism to mitigate the risk of inappropriate technology transfer to China, including but not limited to: assessing the ability of that process to identify students, researchers, and research entities, through a visa disclosure requirement, that are receiving funding from the government of China or an intermediary entity acting in support of China's government.
- Congress amend Internal Revenue Code Section 41 to extend the research and development tax credit to initial stages of deployment for new products, processes, computer software, techniques, formulae, or inventions that increase the production of final and intermediary goods manufactured primarily in the United States. The tax credit should also extend to precompetitive commercial development of basic and applied research per- formed in the United States, particularly in industrial sectors where the People's Republic of China threatens the technological leadership of the United States.
- Congress direct the U.S. Geological Survey, in coordination with the U.S. Department of Energy, U.S. Department of Commerce, U.S. Department of the Interior, and U.S. International Trade Commission to develop and maintain a risk assessment framework that identifies materials used in manufacturing industries critical to both national security and commercial vitality. Such a framework should provide an early warning mechanism for any threats to the U.S. supply of these critical materials, including an increasing concentration of extraction and processing by another country or entity and acquisition of significant mining and processing facilities; increasing export restrictions by another country; large gaps between domestic prices for these materials in another country versus prices on international markets; sharp increases or volatility in price; and substantial control in supply of minerals used within the same industry or related minerals that serve as substitutes by another country.
- Congress direct the National Science Foundation, in coordination with other agencies, to conduct a study on the impact of the activities of Chinese government, state-sponsored organizations, or entities affiliated or supported by the state in international bodies engaged in developing and setting standards for emerging technologies. The study should examine whether standards are being designed to promote Chinese government interests to the exclusion of other participants.

- Congress direct the Office of the Director of National Intelligence to conduct a study on the impact of a Taiwan Strait contingency on the supply of high-technology products to the United States from Taiwan, China, Japan, and South Korea.
- Congress hold hearings examining technologies subject to export controls for mainland China, but not controlled for Hong Kong. These hearings should request that the U.S. Department of Commerce's Bureau of Industry and Security and the U.S. Consulate General in Hong Kong assess the effectiveness of current export controls in preventing unauthorized transshipment to the Mainland or other destinations.

Federal Court Rules Against Suspicionless Searches At Border and In Airports

A U.S. District Court held that U.S. Customs and Border Protection (CPB) and U.S. Immigration and Customs Enforcement's (ICE) current practices for searches of smartphones and computers at the U.S. border are unconstitutional and the agency must have reasonable suspicion before conducting such a search. However, the Court declined the plaintiffs' request that the information taken off of their devices be expunged by the agencies. This ruling follows a Department of Homeland Security Office of the Inspector General (OIG) report that found CPB "did not always conduct searches of electronic devices at U.S. ports of entry according to its Standard Operating Procedures" and asserted that "[t]hese deficiencies in supervision, guidance, and equipment management, combined with a lack of performance measures, limit [CPB's] ability to detect and deter illegal activities related to terrorism; national security; human, drug, and bulk cash smuggling; and child pornography."

In terms of a legal backdrop, the United States Supreme Court has found that searches and seizures of electronic devices at borders and airports are subject to lesser legal standards than those conducted elsewhere in the U.S. under most circumstances. Generally, the government's interest in securing the border against the flow of contraband and people not allowed to enter allow considerable leeway to the warrant requirements for many other types of searches. However, in recent years two federal appeals courts (the Fourth and Ninth Circuits) have held that searches of electronic devices require suspicion on the part of government agents while another appeals court (the Eleventh Circuit) held differently. Consequently, there is not a uniform legal standard for these searches.

The case was brought by the American Civil Liberties Union (ACLU) and the Electronic Frontier Foundation (EFF) on behalf of 10 U.S. citizens and one legal permanent resident who had had their phones and computers searched by CBP or ICE agents upon entering the U.S., typically at airports. The ACLU argued these searches violated the Fourth Amendment's because the agents did not obtain search warrants before conducting the searches of the devices for contraband. The plaintiffs further alleged the searches violated the First Amendment because "warrantless searches of travelers' electronic devices unconstitutionally chill the exercise of speech and associational rights" according to their complaint. The agencies claimed that such searches require neither a warrant nor probable cause and that the First Amendment claim held no water, a position a number of federal appeals courts have held.

The Court noted that

> In January 2018, CBP updated its policy to distinguish between two different types of searches, "basic" and "advanced," and to require reasonable suspicion or a national security concern for any advanced search, but no showing of cause for a basic search. Under

> this policy, an advanced search is defined as "any search in which an officer connects external equipment, through a wired or wireless connection, to an electronic device, not merely to gain access to the device, but to review, copy and/or analyze its contents." The parameters of an advanced search are clearer given this definition than that adopted for a basic search, which is merely defined as "any border search that is not an advanced search." CBP and ICE use the same definitions of basic and advanced searches and ICE policy also requires reasonable suspicion to perform an advanced search.

The Court stated that

> Although the border search exception and the search incident to arrest exception are similar, narrow exceptions to the search warrant requirement, the Court recognizes the governmental interests are different at the border and holds that reasonable suspicion and not the heightened warrant requirement supported by probable cause that Plaintiffs seek here and as applied to the search in Riley is warranted here.

The Court added that

> Moreover, the reasonable suspicion that is required for the currently defined basic search and advanced search is a showing of specific and articulable facts, considered with reasonable inferences drawn from those facts, that the electronic devices contains contraband. Although this may be "a close question" on which at least two Circuits disagree…the Court agrees that this formulation is consistent with the government's interest in stopping contraband at the border and the long-standing distinction that the Supreme Court has made between the search for contraband, a paramount interest at the border, and the search of evidence of past or future crimes at the border, which is a general law enforcement interest not unique to the border.

The Court explained the relief the plaintiffs sought:

- declaration that CPB and ICE's policies violate the First and Fourth Amendment facially and have violated Plaintiffs' First and Fourth Amendment rights by authorizing and conducting searches of electronic devices absent a warrant supported by probable cause, and
- declarations that CPB and ICE's policies violate the Fourth Amendment facially and have violated Plaintiffs' Fourth Amendment rights by authorizing and conducting the confiscation of electronic devices absent probable cause

The Court stated that this relief is granted to the extent that it is declaring "that the CBP and ICE policies for "basic" and "advanced" searches, as presently defined, violate the Fourth Amendment to the extent that the policies do not require reasonable suspicion that the devices contain contraband for both such classes of non-cursory searches and/or seizure of electronic devices; and that the non-cursory searches and/or seizures of Plaintiffs' electronic devices, without such reasonable suspicion, violated the Fourth Amendment."

However, the Court declined to institute a nationwide injunction preventing [CPB and ICE] from "searching electronic devices absent a warrant supported by probable cause that the devices contain contraband or evidence of a violation of immigration or customs laws,"…and b) an injunction preventing Defendants from confiscating electronic devices, with the intent to search the devices after the travelers leave the border, without probable cause and without promptly seeking a

warrant for the search." The Court asserted that briefing on the issues would be needed before such relief could be granted.

ICO Clarifies Special Category Data Handling and Usage

The United Kingdom's (UK) Information Commissioner's Office (ICO) has released guidance designed to help processors and controllers understand their responsibilities regarding "special category data" under the General Data Protection Regulation (GDPR) and the statute the UK enacted to implemented the EU's data protection regime that has additional requirements. Consequently, other EU nations may add requirements on top of those called for by the GDPR.

In its blog posting, the ICO stated "[i]magine if your medical records, information about your sex life or your political opinions were put into the public domain so anyone could see them…[and] [w]hen personal data is shared by mistake the effects can be extremely damaging." The ICO stated that the "GDPR recognises that some types of personal data are very sensitive and states that data controllers must give it extra protection" and these data are "known as special category data." The ICO stated that "[s]pecial category data is information concerning a person's:

- health;
- sex life or their sexual orientation;
- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs; or
- membership to a trade union.

The ICO stated that "[d]ue to the possible risks, the ICO expects controllers to take all necessary precautions to protect this data and we have published new guidance to help you do this."

The ICO explained that Article 9 [of the GDPR] prohibits the processing of special category data. There are 10 exceptions to this general prohibition, usually referred to as 'conditions for processing special category data':

(a) Explicit consent
(b) Employment, social security and social protection (if authorised by law)
(c) Vital interests
(d) Not-for-profit bodies
(e) Made public by the data subject
(f) Legal claims or judicial acts
(g) Reasons of substantial public interest (with a basis in law)
(h) Health or social care (with a basis in law)
(i) Public health (with a basis in law)
(j) Archiving, research and statistics (with a basis in law)

The ICO stated that "[f]ive of the conditions only apply if your processing has an authorisation or basis in EU or member state law…[and] [i]n the UK, this authorisation or basis in law is set out in the Data Protection Act 2018 (DPA 2018.)"

The ICO explained that "[t]he DPA 2018 supplements and tailors the GDPR conditions for processing special category data:

- Section 10 says that if you are relying on a GDPR condition which requires authorisation by law or a basis in law, you must meet one of the additional conditions in Schedule 1.
- Section 11(1) applies to the health or social care condition, and clarifies when the requirement for a professional obligation of secrecy will be met under UK law.
- Schedule 1 Part 1 contains the first four conditions, which give a specific basis in UK law for relying on specific Article 9 conditions:
- employment, social security and social protection - Article 9(2)(b); 2. health or social care - Article 9(2)(h);
- public health - Article 9(2)(i); and
- archiving, research or statistics - Article 9(2)(j).
- Schedule 1 Part 2 then specifies a further 23 potential 'substantial public interest' conditions for the purposes of Article 9(2)(g).
- Schedule 1 (at paragraphs 5 and 38 to 41) also includes additional requirements for you to keep an appropriate policy document and records of processing in relation to special category data.

The ICO stated that "[t]he DPA 2018 does not add any more specific conditions for genetic, biometric or health data, although there is the power for the Secretary of State to make regulations to add or amend conditions."

Warner Letter to HHS On Interoperability and Blocking

Senator Mark Warner (D-VA) pressed the Department of Health and Human Services (HHS) and the Centers for Medicare and Medicaid Services (CMS) to incorporate a number of security features into its proposed rule to increase interoperability and to stop blocking in the electronic health record (EHR) market. In short, Warner is calling on the agency to rewrite and strengthen the rule in ways that would better protect patient data, allow for greater data portability, and foster a more open use of EHR. He contextualized the rule and the issues HHS is grappling with in the context of the larger ongoing debate in Congress about the proper degree of security and privacy for sensitive personal information and the ways the federal government can promote the greatest degree of competition for the public and those entities buying and using technology to share and analyze the data of users.

Warner has introduced a number of bills on technology and serves on a number of committees with jurisdiction over technology issues, giving him a rare vantage on a number of these issues. Warner has also written a number of letters this year to federal agencies and companies regarding the security of their platforms, applications, and data. Most recently, earlier this month, Warner wrote HHS' Office of Civil Rights, the entity charged with policing data security and privacy under Health Insurance Portability and Accountability Act (HIPAA) regulations, regarding reports that "millions of Americans had their private medical images exposed online, due to unsecured picture archiving and communication servers (PACS) that utilize the Digital Imaging and Communications in medicine (DICOM) protocol."

Warner's concerns arose from language in the draft regulations "that would enable third party consumer applications to access sensitive patient and health plan data through application programming interfaces (APIs)." He urged the agencies "to take additional steps to address the potential for misuse of these features in developing the rules around APIs" because "technology providers and policymakers have been unable to anticipate – or preemptively address – the misuse of consumer technology which has had profound impacts across our society and economy." Warner

reiterated his view that "third-party data stewardship is a critical component of information security, and a failure to ensure robust requirements and controls are in place is often the cause of the most devastating breaches of sensitive personal information."

In the notice of proposed rulemaking, HHS and the Office of the National Coordinator for Health Information Technology (ONC) explained that

> This proposed rule would implement certain provisions of the [21st Century Cures Act (P.L. 114-255)], including Conditions and Maintenance of Certification requirements for health information technology (health IT) developers, the voluntary certification of health IT for use by pediatric health providers, and reasonable and necessary activities that do not constitute information blocking. In addition, the proposed rule would implement parts of section 4006(a) of the Cures Act to support patient access to their electronic health information (EHI), such as making a patient's EHI more electronically accessible through the adoption of standards and certification criteria and the implementation of information blocking policies that support patient electronic access to their health information at no cost. Additionally, the proposed rule would modify the 2015 Edition health IT certification criteria and ONC Health IT Certification Program (Program) in other ways to advance interoperability, enhance health IT certification, and reduce burden and costs.

The agencies added

> the proposed rule focuses on establishing Application Programming Interfaces (APIs) for several interoperability purposes, including patient access to their health information without special effort. The API approach also supports health care providers having the sole authority and autonomy to unilaterally permit connections to their health IT through certified API technology the health care providers have acquired. In addition, the proposed rule provides ONC's interpretation of the information blocking definition as established in the Cures Act and the application of the information blocking provision by identifying reasonable and necessary activities that would not constitute information blocking. Many of these activities focus on improving patient and health care provider access to electronic health information and promoting competition.

Warner claimed that "Congress passed the 21st Century Cures Act (P.L. 114-255) with a key objective of improving the protected exchange of electronic health records across the care continuum." He stated that "Section 4003 and 4004 included specific provisions to establish a trusted health information exchange framework and reduce information blocking; it stated that there should be regulation over unreasonable practices to interfere with, prevent, or materially discourage access, exchange, or use of a patient's electronic health records." Warner conceded that HHS "has taken substantial steps to implement fundamental aspects of this legislation" but called for "proper safeguards…to protect patient privacy and sensitive health information." He added that "there should be more work done by HHS to facilitate greater access to, and transfer of, electronic health information that does not inadvertently enable dominant IT providers to leverage their control over user data outside of the health care context into nascent markets for personalized health products."

He noted the similarities of some of the features of the proposed rule and legislation he and other Senators introduced last month. Specifically, he asserted that "[t]he rule is in many ways consistent with bipartisan legislation I have introduced in Congress – the Augmenting Compatibility and

Competition by Enabling Service Switching (ACCESS) Act (S. 2658), which requires our nation's largest social media companies to make user data portable, and make their services interoperable with other platforms." Warner contended that "[c]ommon to both my bill and the proposed rule is a recognition that consumers should have a right to possess their data – and share it with authorized third parties that will protect it." He contended that "[b]oth proposals also seek to address the control over consumer data that incumbents wield, often to the detriment of new, innovative providers." He claimed that "[a]cross all sectors – including health care – innovative products and services, increasingly dependent upon machine learning, rely on user data as the single most important productive input to innovation and customization." Warner stated that "[i]mportantly, however, any approach must balance innovation and ease of access with privacy, security, and a commitment to robust competition…[and] any effort must ensure that such access redounds to the benefit of patients – and that data, once shared with new providers, is not commercialized in ways that benefit those providers without direct benefits or compensation to users."

Warner stated

> In your proposed rule CMS would specifically require Medicare Advantage (MA) organizations, state Medicaid and Children's Health Insurance Program (CHIP) Fee-for-Service (FFS) programs, Medicaid managed care plans, CHIP managed care entities, and qualified health plans (QHPs) on the federally-facilitated exchanges (FFEs) to allow patients to access their personal health information electronically through an open application programming interface (API). Data should be made available through an API so that third party software applications can connect to, process, and make the data available to patients.

Warner stated that "[a]s CMS and HHS move forward with this needed rule – I urge you to include clear standards and defined controls for all stakeholders that ensure third party software applications accessing patient data through APIs are effectively protecting patient information and that patients are appropriately (and routinely) informed, in clear and particularized ways, how their data is used." Warner claimed that "[s]uch standards in a final rule should include at a minimum:

- Patient Access to Data – A guarantee that patients will have ready access to their personal health data and an ability to regularly monitor and ensure the accuracy of such information. Patients should be informed of all commercial uses of their data, including any third parties their data has been shared with (even if it has alleged to have been anonymized). Patients should also have the right to withhold consent for their data to be shared with third parties, or used in new ways without their consent. Patients should also reserve the right to have third party users dispose of their data upon request.
- Adequate Privacy and Security Safeguards – Ensure participating stakeholders can adequately safeguard patient information by using existing best practices for secure storage and complying with applicable breach notification requirements. Moreover, HHS must work with the FTC and state attorneys general to develop mechanisms to report, supervise, and prosecute privacy and security lapses.
- Documentation of the open API specifications and required security controls – Provide clear attestation of the open API specifications as defined for patient data, the security requirements and controls imposed on healthcare providers, and the third-party platform obligations in managing patient data.
- Patient Consent and Terms of Use – CMS and HHS should work proactively with the patient, provider and payer community to ensure users have informed proactive consent when user

data is shared with a third party. In addition – there should be clear protections in place to ensure third party vendors use patient data solely for purposes in which the patient has expressly given informed proactive consent, including cases where patient information may be sold, and that patients retain the right to direct any party that has acquired their data to delete it upon request. Further, those accessing patient data should be prohibited from conditioning continued access on agreement by the patient to share their data with third parties.

Further Reading

- "Meet The Immigrants Who Took On Amazon" – *Wired*. This article traces a burgeoning movement of workers at an Amazon fulfillment center in Minneapolis-St. Paul comprised largely of Somali immigrants to win some concessions from management. The article also traces Amazon's view on unionizing (not surprisingly, it's not favorable) and its employment practices. Whether the efforts of Amazon workers at this warehouse spread to other facilities remains to be seen.
- "Child Abusers Run Rampant as Tech Companies Look the Other Way" – *The New York Times*. A horrific expose on how poorly technology platforms are doing in identifying and taking down child pornography. A number of the tech companies claim security and privacy are the reasons they do not scan the pictures and videos uploaded to their networks, law enforcement officials and other stakeholders decry a lack of will. Worse still, tech companies are not sharing technology to identify this illegal material or are not sharing proprietary methods. Moreover, end-to-end encryption is only complicating matters.
- ""He's F--King Destroyed This Town": How Mark Zuckerberg Became The Most Reviled Man In Tech" – *Vanity Fair*. Once widely admired among the tech community in Northern California, Facebook's CEO is a bit less admired these days on account of the company's bruising (some say illegal) business tactics and how its actions portray the larger tech world.
- "Yes, Robots Are Stealing Your Job" – *The New York Times*. Candidate for the Democratic nomination for president, Andrew Yang, shares his views on automation and why many current and future jobs may soon not be available for humans. He discusses his proposal on how to help those displaced by the coming wave of automation, including a universal basic income.
- "How Facebook's 'Switcheroo' plan concealed scheme to kill popular apps" – *ComputerWeekly.com*. An investigative journalist got his hands on thousands of pages of documents showing Facebook's methods of dealing with competitors and potential rivals, which a former app developer is alleging in a California state court violates antitrust laws. In addition to the outlets reporting on these documents, the cache of internal Facebook communications have been provided to the House Judiciary Committee for its investigation into digital markets.
- "Microsoft vows to 'honor' California's sweeping privacy law across entire US" – *The Verge*. Just as with the GDPR, Microsoft says it will voluntarily honor the "core" principles of the CCPA when it becomes effective.